08.06.2022



| **Vorsitz**: | **Protokoll**: |
|---|---|
| Friedrich Rubner<br>Telefon +49 173-6895533<br>Leiter Arbeitsfeld MSR-Technik<br>friedrich.rubner@euroapi.com | Sven Seintsch<br>Telefon +49 173-2317312<br>Leiter Arbeitsfeld Prüftechnik<br>sven.seintsch@bilfinger.com |



**IGR Positionspapier**

**Parametrierung / Bedienung von Feldgeräten mittels Smartphone und Tablet**

Derzeit erscheinen auf dem Feldgeräte-Markt neue Geräte die mittels Webserver und/oder Apps drahtlos (z.B. via Bluetooth) bedient werden können. Im Gegensatz zu standardisierten Wireless-Technologien wie z.B. Wireless HART, fehlen hier Standards im Sinne der Anwender.
Diese neue Geräte-Generation ist derzeit völlig offen gestaltet, sie bietet die Möglichkeit der Kommunikation mit Feldgeräten über Geräte aus dem Consumer Markt, wie Tablets oder Smartphones. Damit eröffnen sich ganz neue Angriffsflächen zur Manipulation von Gerätedaten in den Feldgeräten.
Als Beispiel sollen hier genannt werden:
- Veränderungen am Gerät mittels App ohne Datenkonsistenz im Automatisierungssystem
- Veränderungen am Gerät durch nicht autorisierte Personen
- Unklarer Umgang mit Apps, geliefert von Drittanbietern (ohne Validierung)

Dem Anlagenbetreiber soll neben den möglichen Vorteilen (z. B. Auslesen von Geräteinformationen), die Gefahren verdeutlicht werden um ihn in die Lage zu versetzen Maßnahmen zu ergreifen, die einen ordnungsgemäßen Betrieb der Anlage auch zukünftig sicherstellen können.

1. **Themen-Beschreibung**
2. **Anforderungen**
3. **Fazit**

## 1. Themen-Beschreibung

Bislang existieren für Feldgeräte keine herstellerübergreifenden Regularien bei Verwendung dieser Technologien. Es ist auch nicht auszuschließen, dass durch Drittanbieter Bedienungssoftware auf den Markt gelangt die Parameterzuweisungen unvollständig oder falsch vornehmen oder die aktuellen Softwarestände der Geräte nicht berücksichtigt.
Aus Anwendersicht ist eine Standardisierung der Schnittstelle und Bedienoberfläche dringend erforderlich. Ebenso ist die Funktion, wie auch die Funktionalität dieses Datenkanals festzulegen. Zum Beispiel:

- nur lesend
- lesend und schreibend
- lesend und schreibend (Freigabe, Bedarf, Dateninhalte)

## 2. Anforderungen

Der sichere und geregelte Betrieb muss auch mit dieser neuen Technologie sichergestellt bleiben. Zurzeit ist diese Problematik nicht gelöst, herstellerübergreifende Vereinbarungen fehlen.

Die im Folgenden aufgeführten Anwender-Anforderungen spiegeln den jetzigen Erkenntnisstand wieder und sind beispielhaft und nicht vollständig.

### 2.1. Bedienung

Bei den derzeit eingeführten Technologien (4-20mA, Feldbus, Wireless HART) ist die Auswahl des Gerätes durch die Bedienung von Hand vor Ort oder durch den Anschluss eines Parametriergerätes sichergestellt und die Parametrierung ist durch ein Passwort im Gerät geschützt. Dies setzt intensive Kenntnisse des Gerätes und Parametriergerätes voraus.

➔ Die alleinige Verwendung eines Passwortes bei der neuen Technologie als Zugriffsschutz zur Parametrierung vor Ort ist nicht ausreichend.

#### 2.1.1 Geräteauswahl / Identifikation

➔ Ein einheitlicher Verbindungsaufbau (herstellübergreifend) mit Identifikation des Gerätes und einer Anmeldeprozedur ist notwendig.
➔ Es ist sicherzustellen, dass nur das Gerät parametriert bedient wird dass der Anwender ausgewählt hat.
➔ Es muss eindeutig erkennbar sein, ob das richtige Gerät ausgesucht und angesprochen wird, dazu ist beim Verbindungsaufbau die TAG-Nummer und die Seriennummer zu übertragen.
➔ Bei der Identifizierung muss auf doppelt vergebene TAG-Nummern bzw. auf unterschiedliche Seriennummer bei gleichen TAG geprüft und gewarnt werden.
➔ Es darf keine Parametrierung nicht gewünschter Geräte erfolgen.
➔ Es muss sichergestellt sein, dass immer nur ein Gerät bedient wird.
➔ Es muss beim Verbindungsaufbau eine Prüfung erfolgen, dass die Software am Gerät auch mit der verwendeten Bedien-Software kompatibel ist. Eine Bedienung darf bei Inkompatibilität nicht möglich sein.

### 2.1.2 Passwortschutz zur Parametrierung

- ➔ Die Vergabe eines individuellen Passwortes je Gerät ist erforderlich.
- ➔ Die bisher erfüllten Voraussetzungen zur Sicherstellung der Zugriffsrechte darf durch drahtlose Kommunikation nicht unterlaufen werden.
- ➔ Ein einheitliches Zugangskonzeptes (Passwort, Masterpasswort, Zugangsmöglichkeit nach Verlust des Passwortes (PIN/PUK)) – z.B. Eingabe der Seriennummer mit Masterpasswort.
- ➔ Insbesondere darf das Masterpasswort nicht frei verfügbar sein (z.B. in der Gerätedokumentation)

## 2.2. Konsistenz der Daten

Datensätze im Gerät und im Leitsystem/Bedienprogramm und in der Spezifikation müssen übereinstimmen (Betreiberspezifikation). Insbesondere muss die Übereinstimmung auch bei Änderungen vor Ort durchgängig gleich sein.

- ➔ Datenveränderungen müssen ersichtlich sein: wann, wo, wer, wie.
- ➔ Änderungs-Merker mit Datum bei Veränderung von Parametern.
- ➔ Abgleich der Parameter mit der Engineering-Station und der Datenbank des Leitsystems.

## 2.3. Bedienoberflächen

Zurzeit entwickelt jeder Hersteller eine eigene App mit eigenen Ansichten und Parameternamen, Identifikation und Zugriffsrechten.

- ➔ Bedienoberflächen der Apps müssen die gleiche Bedienlogik aufweisen wie das zu parametrierende Gerät (Ebenen-Modell). Das gilt auch für die Bedienoberfläche der App/Webserver und auch bezüglich der Darstellung im Bedienprogramm des Leitsystems.
- ➔ Unabhängig vom Gerät, dem SW-Stand, dem Betriebssystem des jeweiligen Bediengerätes müssen die Bedienoberflächen der Apps gleich sein.
- ➔ Zur Bezeichnung der Parameter sind die NAMUR-Parameternamen gemäß NE131 zu verwenden.
- ➔ Ein Styleguide für Webeserver und Apps ist vorzusehen. Z.B. FDI Styleguide.

## 2.4. Betriebssysteme

Die Betriebssysteme dürfen keinen Einfluss auf die Übertragung von Daten und Parameterwerten haben.

- ➔ Je nach Betriebssystem und Version des Betriebssystems müssen Apps zur Verfügung stehen und aktualisiert werden.
- ➔ Die Anzahl der Apps ist zu minimieren damit der Pflegeaufwand möglichst gering bleibt.
- ➔ Die Auf- und Abwärtskompatibilität mit verschiedenen Betriebssystemversionen muss gewährleistet sein.

### 2.5. Schnittstellen

Zu den bisherigen Standards in der Signal- und Daten-Übertragung (4-20mA, HART, Profibus) kommen mit der drahtlosen Kommunikation weitere Standards (Bluetooth, NFC, WLAN, IR, …) hinzu, für die es derzeit in der Feldgerätekommunikation keinen Standard gibt.

- ➔ Beschränkung auf eine Technologie/Standard in der drahtlosen Kommunikation.
- ➔ Reichweiten müssen so begrenzt sein, dass für den Bediener das zu bedienende Gerät im Nahbereich bleibt.
- ➔ Die Geräte sind konstruktiv so aufzubauen, dass der Anwender die Möglichkeit hat die drahtlose Kommunikation auszuschalten, z.B. durch Entfernung der Hardware oder Schalter.
- ➔ Im Auslieferungszustand ist die drahtlose Kommunikation abgeschaltet.

### 2.6. Drittanbieter von Apps

Bisher bieten nur Gerätehersteller Apps für ihre Geräte an.

- ➔ Drittanbieter müssen sich an die Standards der Geräte-Hersteller halten.
- ➔ Die Geräte-Hersteller sind verantwortlich für die Validierung.

### 2.7. Mögliche Risiken

- ➔ Unbeabsichtigte Veränderung der spezifizierten Funktionalität/Parameter eines Gerätes, die teilweise auch in Sicherheitsbetrachtungen beschrieben sein können. Dazu zählen Messbereich, Ansprechverhalten, Störverhalten und weitere Parameter.
- ➔ Bei Nichtbeachtung der obigen Forderungen kann durch drahtlose Kommunikation in Zukunft jedes Smartphone oder Tablett eine Manipulation am Gerät durchführen, da eine direkte Verbindung zum Gerät nicht erforderlich ist.
- ➔ Es fehlt ein Sicherungskonzept für Datenübertragung, welches auch die Zugehörigkeit der Daten zum jeweiligen Gerät feststellt.
- ➔ Es ist sicherzustellen, dass kein Gerät von außerhalb der Anlage bedient werden kann.
- ➔ Bediengerät und Feldgerät sind eindeutig miteinander zu verknüpfen. Diese Aktivierung muss auf beiden Geräten aktiv bestätigt werden, nur dann darf eine Kommunikation möglich sein.

## 3. Fazit

Es wird empfohlen, Geräte mit drahtloser Kommunikation nur zum Auslesen von Daten und Parametern zu verwenden. Das Schreiben von Parametern muss ausgeschlossen sein. Eine eindeutige Geräteidentifikation muss sichergestellt sein.